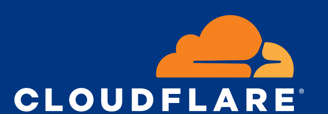
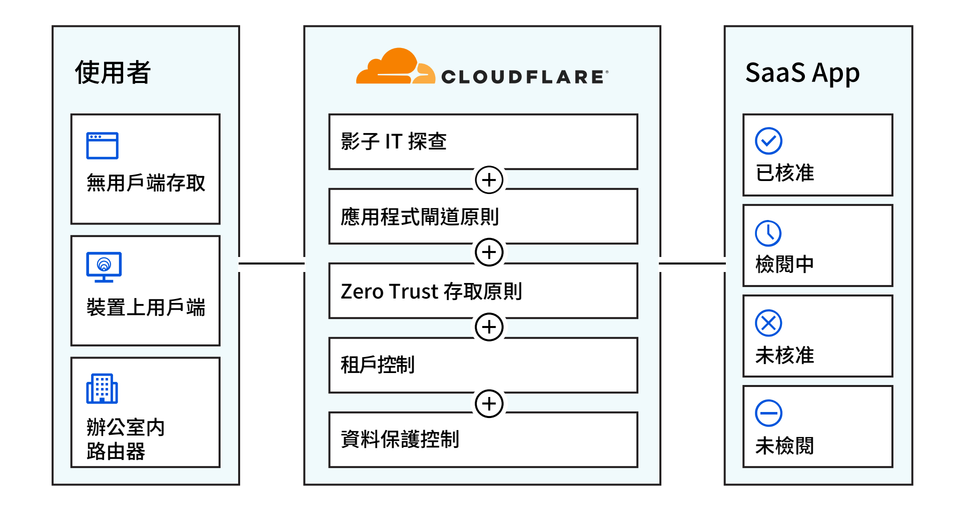
解決方案簡述



對每一個 SaaS 應用程式的 Zero Trust 可見性和可控性

SaaS 應用程式可讓您的團隊執行比以往更多的作業，但它們為工作團隊提供靈活性和自由的同時，也為企業帶來安全性風險、可見度挑戰和存取控制障礙。

Cloudflare 為您提供保護資料和工作團隊所需的工具，同時仍然允許員工使用可助其完成工作的工具。



探索和控制 Shadow IT

如果無法深入瞭解員工正在使用的應用程式，您就無法控制如何儲存、分享或向第三方公開敏感性資料。Cloudflare 有助於您探索、分類和控制企業內所有已核准和未核准的應用程式，在同一集中位置記錄每一次連線和每一項要求。



套用 Zero Trust 存取機制

SaaS 應用程式託管在公司網路外部，導致您的資安團隊難以控制使用者如何存取這些應用程式並將資料移入和移出這些應用程式。Cloudflare 在 SaaS 應用程式之前採用 Zero Trust 安全性措施，對合法使用者進行驗證，並防止未經授權的使用者或風險裝置存取您的檔案和資料。

使用者和資料保護控制措施

當員工存取錯誤的應用程式執行情景時，他們可能會在非認可地點分享和儲存您的資料，為潛在資料洩漏和其他安全性風險大開方便之門。Cloudflare 可協助您控制分享和儲存資料，無論該資料正透過網路傳輸，還是在我們遠端瀏覽器內使用。現在，您可以構建和部署 Zero Trust 瀏覽機制，以保護位於任何 SaaS 應用程式內的資料，同時讓您的員工無法存取錯誤的應用程式或已核准應用程式給予了錯誤的使用者。

探索和控制Shadow IT

評估員工使用的應用程式

如果您的 IT 團隊看不到員工正在使用的應用程式，就無法控制對這些應用程式內資料所執行的作業。Cloudflare 按應用程式類型彙整我們活動記錄中的所有 HTTP 要求，並自動進行分類從中，您可以設定狀態並追蹤整個企業內已核准和未核准應用程式的使用情況。

記錄每一次連線和每一項要求

Cloudflare 有助於紓解員工存取未經批准應用程式或使用未授權裝置存取敏感性資訊時所帶來的企業的風險。會在同一集中位置記錄每一次連線和每一項要求，以便您查看正在使用的應用程式及使用者在這些應用程式內執行的動作。管理員還能封鎖和允許對 SaaS 應用程式的要求，防止使用者繞過重要安全控制機制，未經授權地存取企業內的應用程式、資源和資料。

主要功能

- 自動追蹤已受 Cloudflare 保護的應用程式
- 在 Cloudflare 網路中保留日誌長達 6 個月
- 將日誌推送至一或多個雲端日誌儲存體和 SIEM 服務

Analytics

Access

Last 7 days

Export

Shadow IT Discovery

Approved Unapproved In review Unreviewed

Unique application users

Review All

70 60 50 40 30 20 10 0

SUNDAY MONDAY TUESDAY WEDNESDAY THURSDAY FRIDAY SATURDAY

Top approved applications View more

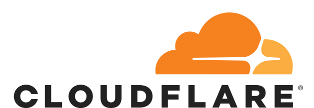
Asana	1,352
GChat	1,405
Slack	254
Google Cloud	98

Unique user accounts found in Gateway

Top unapproved applications View more

Slack	254
Discord	49
Microsoft Teams	48
Pinterest	37

Unique user accounts found in Gateway



將 Zero Trust 存取機制套用至 SaaS 應用程式

透過 Cloudflare 身分識別代理提供安全 SaaS 存取

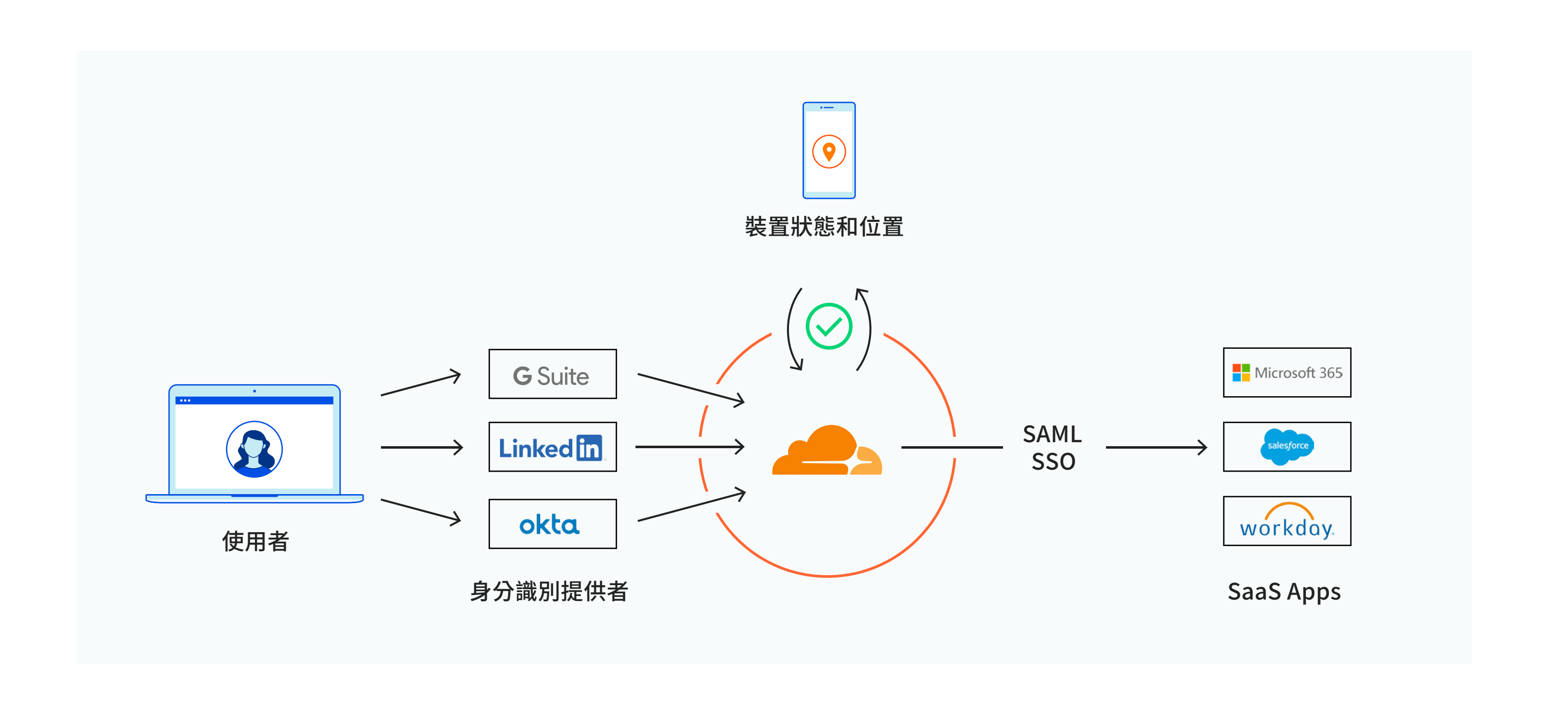
SaaS 應用程式由第三方託管，通常由業務單位進行管理，這意味著您的 IT 團隊幾乎無法掌控使用者如何存取這些應用程式。Cloudflare 位於您的身分識別提供者和 SaaS 應用程式之間，支援您構建身分識別確認和內容導向 Zero Trust 規則，並將其套用至登入程序，而且不會影響終端使用者體驗。

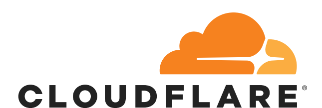
為使用者裝置決定應用程式權限

您的 IT 部門需要對企業管理的裝置登入 SaaS 應用程式方式進行精細管控。Cloudflare 將 Zero Trust 規則套用在單一登入程序，所有應用程式可透過 SAML 格式得以驗證支援。使用者先向其身分識別提供者進行驗證；然後，Cloudflare 會依據裝置狀態和位置檢查要求，然後再授予對任何 SaaS 應用程式的存取權限，並透過彈性工作階段管理進行持續驗證。安全性管理員亦可建立特定於裝置的機制。如此一來，使用者只能透過滿足預先建立的安全性要求（包括 mTLS 憑證）的裝置存取應用程式。

主要功能

- 整合多個身分識別提供者或同一提供者的多個執行情景
- 使用特定於應用程式的機制（例如，MFA 需要硬體）驗證使用者身分
- 使用特定於應用程式的規則（例如已執行 SWG 原則、已安裝 EPP、mTLS 憑證、已啟用磁碟加密）和位置來驗證裝置狀態
- Cloudflare 應用程式啟動器入口網站，可允許使用者查看和存取所有已核准的 SaaS 應用程式





將使用者和資料保護控制機制套用至任何SaaS 應用程式

限制對非企業應用程式執行情景的存取

Cloudflare 支援透過 HTTP 閘道機制控制使用用戶，可以設定這些機制以防止使用者存取應用程式的版本。Cloudflare 並非透過企業 VPN 使用內部部署代理伺服器來執行這些機制，而是透過大型全球資料中心網路來篩選和檢查所有流量和要求。因此，您的使用者永遠不會遇到等待時間增加或效能下降的情況。

防止企業資料離開您的使用用戶

Cloudflare 可讓您輕鬆構建和部署 Zero Trust 瀏覽機制，控制和保護 Web 式應用程式內的資料。所有應用程式代碼都在安全的遠端瀏覽器中執行，該瀏覽器透過我們龐大的全球網路遠端執行，而非在端點裝置上執行。因此，可以保護敏感性資料，不用受到入侵、被不受信任的裝置存取和zero-day 威脅。管理員仍可控制使用者如何存取和分享該資料，以便您能將意外資料丟失或更嚴重的資料外洩風險降至最低。

主要功能

- 基於多個條件允許或封鎖瀏覽器行為，包括應用程式、應用程式類型、主機名稱、使用者身分和安全性風險
- 控制使用者在瀏覽器內的動作：下載、上傳、複製/貼上、鍵盤輸入和列印功能

CLOUDFLARE

控制檔案下載/上傳

封鎖複製/黏貼和列印

可在無頭瀏覽器內控制
不可信的互動

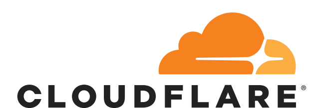
Zero Trust
繪製命令

不可信互動

使用者瀏覽器

敏感性資料

任何 Web App



Cloudflare 的獨特優勢



平台涵蓋廣度

Cloudflare 在您的 SaaS 應用程式之前實施 Zero Trust 存取 (ZTNA)、閘道 (SWG) 和隔離瀏覽器控制措施，而無需您的 IT 團隊設定和運行專用 CASB 產品。



從零開始構建

Cloudflare 的 CASB 功能可與我們 ZTNA、SWG 和 RBI 服務順暢合作，因為所有功能都是從零開始構建，無需兼顧多個單一功能產品來保護您的應用–程式和團隊。



單一控制面板

Cloudflare 允許組織從單一儀表板設定原則和管理應用程式的存取與使用情況，以便您可以迅速監控所有要求和權限。

Cloudflare 可協助團隊透過原生整合的 Zero Trust 安全性功能套件，監控、保護和控制 SaaS 應用程式。

立即瞭解更多